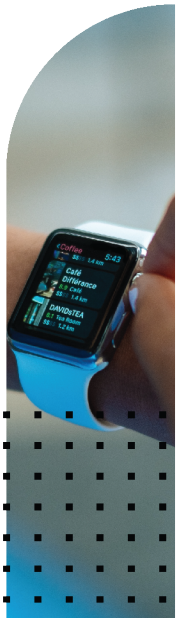
Release Notes

FortiAuthenticator 6.4.4



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

June 29, 2022
FortiAuthenticator 6.4.4 Release Notes
23-644-813499-20220629

TABLE OF CONTENTS

Change log

Date	Change Description
2022-06-03	Initial release.
2022-06-15	Updated Product integration and support on page 14.
2022-06-29	Updated Maximum values for hardware appliances on page 23.

FortiAuthenticator 6.4.4 release

This document provides a summary of new features, enhancements, support information, installation instructions, caveats, and resolved and known issues for FortiAuthenticator 6.4.4, build 1028.

FortiAuthenticator is a user and identity management solution that provides strong authentication, wireless 802.1X authentication, certificate management, RADIUS AAA (authentication, authorization, and accounting), and Fortinet Single Sign-On (FSSO).

For additional documentation, please visit: https://docs.fortinet.com/product/fortiauthenticator/

Special notices

TFTP boot firmware upgrade process

Upgrading FortiAuthenticator firmware by interrupting the FortiAuthenticator boot process and installing a firmware image from a TFTP server erases the current FortiAuthenticator configuration and replaces it with factory default settings.

Monitor settings for GUI access

Fortinet recommends setting your monitor to a screen resolution of 1600x1200. This allows for all the objects in the GUI to be viewed properly without the need for scrolling.

Before any firmware upgrade

Save a copy of your FortiAuthenticator configuration before upgrading the firmware. From the administrator dropdown menu in the toolbar, go to **Restore/Backup**, and click **Download Backup File** to backup the configuration.

After any firmware upgrade

Clear your browser cache before logging in to the FortiAuthenticator GUI to ensure the pages display properly.

FortiAuthenticator does not support PEAP-MAB

FortiAuthenticator only supports MAB in clear-text and not the encapsulated MAB.

What's new

FortiAuthenticator version 6.4.4 includes the following enhancement:

New encryption/decryption key field in the backup and restore related REST API endpoint

The `recovery` endpoint now includes the `key` field. See the REST API Solutions Guide.

Zero trust tunnels

FortiAuthenticator introduces zero trust tunnels. FortiAuthenticator can form a zero trust tunnel (SSLVPN) to a remote zero trust server, e.g., a FortiGate.

The tunnels allow FortiAuthenticator to securely access TCP-based-on-premise services from the public internet.

Also, you can configure zero trust tunnels to access on-premise LDAP/AD server.

A new **Zero Trust Tunnels** tab in **System > Network** to configure zero trust tunnels.

A new **Use Zero Trust tunnel** toggle when creating or editing an LDAP server in **Authentication > Remote Auth. Servers > LDAP** to configure a remote LDAP server to use a zero trust tunnel.

If zero trust tunnel is enabled for the secondary server:

- FortiAuthenticator attempts to connect to the primary server. If zero trust is enabled for the primary server, then FortiAuthenticator uses zero trust tunnel associated with the primary server.
- When FortiAuthenticator is unable to reach the primary server, then FortiAuthenticator attempts to use the secondary server. FortiAuthenticator uses the zero trust tunnel associated with the secondary server.

The following actions now generate log events in FortiAuthenticator:

- Bring up a zero trust tunnel
- Bring down a zero trust tunnel
- Unable to bring up a zero trust tunnel

FortiMail integration

When creating or editing local and remote user accounts in **Authentication > User Management**, the following new fields are included in the **User Information** pane:

- **Birthdate**
- **Company**

- **Department**
- **Display name**
- **Postal code** (only in local user accounts)
- **Title**

The CSV file based import/ export of local users uses a new format.

Remote user sync rules in **Authentication > User Management** now include the following new fields in the **LDAP User Mapping Attributes** pane:

- **Company**
- **Department**
- **Display name**
- **Title**

The LDAP server configured in **Authentication > LDAP Service** now offers the following attributes for the users in its directory:

- **alternatemail:** String of comma-separated email addresses from the "Alternative email addresses" table
- **birthdate:** Birthdate field
- **company:** Company field
- **c**: Country
- **custom1:** Custom1 field
- **custom2:** Custom2 field
- **custom3:** Custom3 field
- **department:** Department field
- **displayname:** Display name field
- **l**: City or local (e.g. Burnaby)
- **mobiletelephonenumber:** Mobile number field
- **postaladdress:** String of aggregated address fields in the format: "<Street address>, <City>, <State/Province> <Zip/Postal code> <Country>"
- **postalCode**: Postal or zip code
- **st**: State or province (e.g. BC)
- **street**: street address (e.g. 4190 Still Creek Dr.)
- **telephonenumber**: Phone number field
- **title:** Title field

For the LDAP server, FortiAuthenticator now supports password changes in compliance with RFC 3062

New SNMP related endpoints

New `snmpgeneral`, `snmp`, and `snmp/[id]/hosts` endpoints. See REST API Solutions Guide.

Client certificate authentication for SMS gateways

A new **Client Certificate** authorization type for TLS connection in **System > Messaging > SMS Gateways** when creating or editing an SMS gateway.

Admin can configure any OTP delivery method

When creating or editing a local or remote user, the administrator can now specify the source of tokens using the new **Deliver token codes from** option in **One-Time Password (OTP) authentication**.

Previously available options in **One-Time Password (OTP) authentication** are available when **Deliver token codes from** is set as **FortiAuthenticator**.

When **Deliver token codes from** is set as **FortiToken Cloud**, the administrator can now specify token delivery options.

A new **Show delivery options** option to show the token code delivery options when editing a local or remote user account with FortiToken Cloud OTP enabled.

When creating or editing a remote user sync rule in **Authentication > User Management > Remote User Sync Rules**, FortiAuthenticator now offers the following FortiToken Cloud options in the **Synchronization Attributes** pane:

- **FortiToken Cloud- Default**
- **FortiToken Cloud- FortiToken Mobile**
- **FortiToken Cloud- FortiToken Hardware**
- **FortiToken Cloud- Email**
- **FortiToken Cloud- SMS**

FortiToken Cloud: Sync all remote user account changes

FortiAuthenticator updates FortiToken Cloud when a remote user configured for FortiToken Cloud MFA is updated.

The following updates to the remote user configuration are synced to FortiToken Cloud:

- Existing remote FortiAuthenticator user with FortiToken Cloud MFA configured is deleted from FortiAuthenticator.
- Existing remote FortiAuthenticator user with FortiToken Cloud MFA configured has an email address change.
- Existing remote FortiAuthenticator user with FortiToken Cloud MFA configured has a mobile number change.

The above applies to all FortiAuthenticator remote users, including remote users modified or deleted as a result of changes in the remote user synchronization rules.

Upgrade instructions

Back up your configuration before beginning this procedure. While no data loss should occur if the procedures below are correctly followed, it is recommended a full backup is made before proceeding and the user will be prompted to do so as part of the upgrade process.

For information on how to back up the FortiAuthenticator configuration, see the FortiAuthenticator Administration Guide.

Hardware and VM support

FortiAuthenticator 6.4.4 supports:

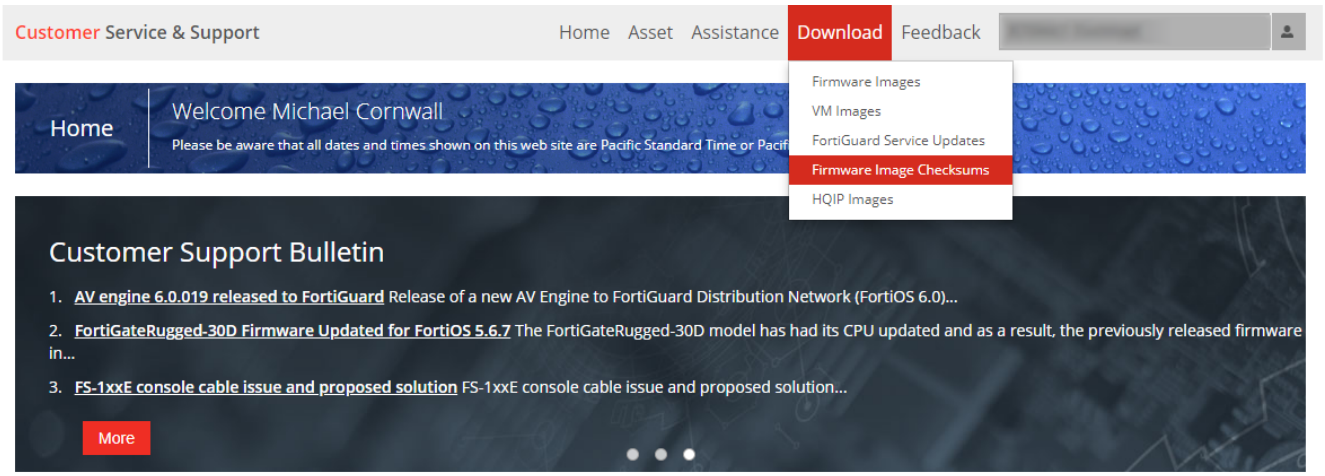
- FortiAuthenticator 200D
- FortiAuthenticator 200E
- FortiAuthenticator 300F
- FortiAuthenticator 400C
- FortiAuthenticator 400E
- FortiAuthenticator 1000D
- FortiAuthenticator 2000E
- FortiAuthenticator 3000D
- FortiAuthenticator 3000E
- FortiAuthenticator 800F
- FortiAuthenticator VM (VMWare, Hyper-V, KVM, Xen, Azure, AWS, Oracle OCI, and Alibaba Cloud)

Image checksums

To verify the integrity of the firmware file, use a checksum tool to compute the firmware file's MD5 checksum. Compare it with the checksum indicated by Fortinet. If the checksums match, the file is intact.

MD5 checksums for software releases are available from the Fortinet Support website.

Customer service and support image checksum tool



After logging in to the web site, in the menus at the top of the page, click **Download**, then click **Firmware Image Checksums**.

In the **Image File Name** field, enter the firmware image file name including its extension, then click **Get Checksum Code**.

Upgrading from FortiAuthenticator 4.x/5.x/6.x

FortiAuthenticator 6.4.4 build 1028 officially supports upgrades from previous versions by following these supported FortiAuthenticator upgrade paths:

- If currently running FortiAuthenticator 6.0.5 or older, first upgrade to 6.0.7, then upgrade to 6.4.4, else the following message will be displayed: `Image validation failed: The firmware image model number is different from the appliance's.`
- If currently running FortiAuthenticator 6.0.7, then upgrade to 6.4.4 directly.
- If currently running FortiAuthenticator between 6.1.0 and 6.2.0, first upgrade to 6.3.3, then upgrade to 6.4.4.
- If currently running FortiAuthenticator 6.2.1 or later, then upgrade to 6.4.4 directly.

When upgrading existing **KVM** and **Xen** virtual machines to FortiAuthenticator 6.4.4 from FortiAuthenticator 6.0.7, you must first increase the size of the virtual hard disk drive containing the operating system image (not applicable for AWS & OCI Cloud Marketplace upgrades). See Upgrading KVM / Xen virtual machines on page 12.

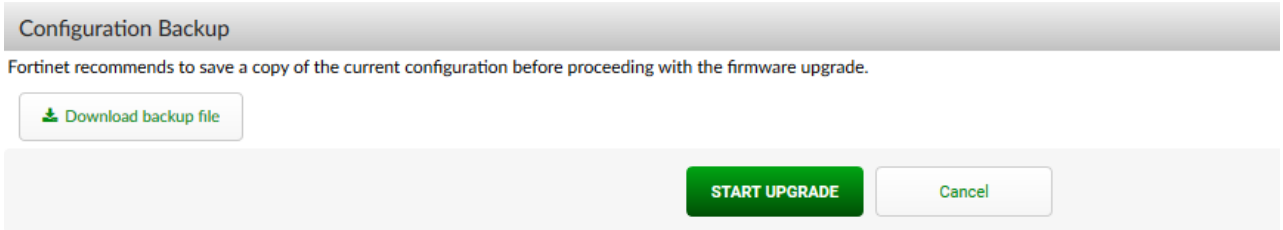
Upgrade to and from FortiAuthenticator 6.0.6 is not recommended.

Firmware upgrade process

First, back up your configuration, then follow the procedure below to upgrade the firmware.

Before you can install FortiAuthenticator firmware, you must download the firmware image from the Fortinet Support website, then upload it from your computer to the FortiAuthenticator unit.

1. Log in to the Fortinet Support website. In the **Download** section of the page, select the **Firmware Images** link to download the firmware.
2. To verify the integrity of the download, go back to the **Download** section of the login page and click the **Firmware Image Checksums** link.
3. Log in to the FortiAuthenticator unit's web-based manager using the **admin** administrator account.
4. Upload the firmware and begin the upgrade.
   When upgrading from FortiAuthenticator 6.0.4 and earlier:
   a. Go to **System > Dashboard > Status**.
   b. In the **System Information** widget, in the **Firmware Version** row, select **Upgrade**. The **Firmware Upgrade or Downgrade** dialog box opens.
   c. In the **Firmware** section, select **Choose File**, and locate the upgrade package that you downloaded.
   When upgrading from FortiAuthenticator 6.1.0 or later.
   a. Click on the administrator name in the upper-right corner of the GUI to display the dropdown menu, and click **Upgrade**.
   b. In the **Firmware Upgrade or Downgrade** section, select **Upload a file**, and locate the upgrade package that you downloaded.
5. Select **OK** to upload the file to the FortiAuthenticator.
   Your browser uploads the firmware file. The time required varies by the size of the file and the speed of your network connection. When the file transfer is complete, the following message is shown:



   It is recommended that a system backup is taken at this point. Once complete, click **Start Upgrade**.
   Wait until the unpacking, upgrade, and reboot process completes (usually 3-5 minutes), then refresh the page.

Due to a known issue in 6.0.x and earlier releases, the port5 and port6 fiber ports are inverted in the GUI for FAC-3000E models (i.e. port5 in the GUI corresponds to the physical port6 and vice-versa).

This is resolved in 6.1.0 and later, however, the upgrade process does not swap these configurations automatically. If these ports are used in your configuration during the upgrade from 6.0.x to 6.1.0 and later, you will need to physically swap the port5 and port6 fibers to avoid inverting your connections following the upgrade.

Upgrading KVM / Xen virtual machines

When upgrading existing KVM and Xen virtual machines from FortiAuthenticator 6.0.7 to 6.4.4, it is necessary to manually increase the size of the virtual hard disk drive which contains the operating system image before starting the upgrade. This requires file system write-access to the virtual machine disk drives, and must be performed while the virtual machines are in an offline state, fully powered down.

If your virtual machine has snapshots, the resize commands detailed below will exit with an error. You must delete the snapshots in order to perform this resize operation. Please make a separate copy of the virtual disk drives before deleting snapshots to ensure you have the ability to rollback.

Use the following command to run the resize on KVM:

```
qemu-img resize /path/to/fackvm.qcow2 1G
```

Use the following command to run the resize on Xen:

```
qemu-img resize /path/to/facxen.qcow2 1G
```

After this command has been completed, you may proceed with the upgrade from 6.0.7 to 6.4.4

Recovering improperly upgraded KVM / Xen virtual machines

If the upgrade was performed without completing the resize operation above, the virtual machine will fail to properly boot, instead displaying many **initd** error messages. If no snapshots are available, manual recovery is necessary.

To recover your virtual machine, you will need to replace the operating system disk with a good copy, which also requires write-access to the virtual hard disks in the file system while the virtual machines are in an offline state, fully powered down.

To recover an improperly upgraded KVM virtual machine:

1. Download the 6.0.7 GA ZIP archive for KVM, **FAC_VM_KVM-v6-build0059-FORTINET.out.kvm.zip**.
2. Extract the archive, then replace your virtual machine's **fackvm.qcow2** with the one from the archive.
3. Execute the following command:
   ```
   qemu-img resize /path/to/fackvm.qcow2 1G
   ```

To recover an improperly upgraded Xen virtual machine:

1. Download the 6.0.7 GA ZIP archive for Xen, **FAC_VM_XEN-v6-build0059-FORTINET.out.xen.zip**.
2. Extract the archive, then replace your virtual machine's **facxen.qcow2** with the one from the archive.
3. Execute the following command:
   ```
   qemu-img resize /path/to/facxen.qcow2 1G
   ```

Product integration and support

Web browser support

The following web browsers are supported by FortiAuthenticator 6.4.4:

- Microsoft Edge version 101
- Mozilla Firefox version 100
- Google Chrome version 102

Other web browsers may function correctly, but are not supported by Fortinet.

FortiOS support

FortiAuthenticator 6.4.4 supports the following FortiOS versions:

- FortiOS v7.2.x
- FortiOS v7.0.x
- FortiOS v6.4.x
- FortiOS v6.2.x
- FortiOS v6.0.x

Fortinet agent support

FortiAuthenticator 6.4.4 supports the following Fortinet Agents:

- FortiClient v.6.x , v.7.x for Microsoft Windows and macOS (Single Sign-On Mobility Agent)
- For FortiAuthenticator Agents for Microsoft Windows and Outlook Web Access compatibility with FortiAuthenticator, see the *Agents Compatibility Matrix* on the Fortinet Docs Library.
- FSSO DC Agent v.5.x
- FSSO TS Agent v.5.x

Other Agent versions may function correctly, but are not supported by Fortinet.

For details of which operating systems are supported by each agent, please see the install guides provided with the software.

Note: FortiAuthenticator Agent for Microsoft Windows 4.0 and above required to support emergency offline access. Also, FortiAuthenticator Agent for Microsoft Windows below 4.0 compatible for all other features.

Virtualization software support

FortiAuthenticator 6.4.4 supports:

- VMware ESXi / ESX 6/7
- Microsoft Hyper-V 2010, Hyper-V 2012 R2, Hyper-V 2016, and Hyper-V 2019
- Linux Kernel-based Virtual Machine (KVM) on Virtual Machine Manager and QEMU 2.5.0
- Xen Virtual Machine (for Xen HVM)
- Nutanix
- Amazon AWS
- Microsoft Azure
- Oracle OCI
- Alibaba Cloud

Support for HA in Active-Passive and Active-Active modes has not been confirmed on the FortiAuthenticator for Xen VM at the time of the release.

See FortiAuthenticator-VM on page 16 for more information.

Third-party RADIUS authentication

FortiAuthenticator uses standards based RADIUS for authentication and can deliver two-factor authentication via multiple methods for the greatest compatibility:

- RADIUS Challenge Response - Requires support by third party vendor.
- Token Passcode Appended - Supports any RADIUS compatible system.

FortiAuthenticator should therefore be compatible with any RADIUS capable authentication client / network access server (NAS).

FortiAuthenticator-VM

For information about FortiAuthenticator-VM deployments and system requirements, see the VM installation guide on the Fortinet Docs Library.

Resolved issues

The resolved issues listed below may not list every bug that has been corrected with this release. For inquiries about a particular bug, please visit the Fortinet Support website.

Bug ID	Description
706701	FortiAuthenticator cluster is inconsistently accessible via HA interfaces from outside the HA subnet.
725800	IAM username validation not consistent in REST API.
755551	FortiAuthenticator - [Third Party] Apache Http_Server -- Precaution Upgrade.
757516	Local user CSV export does not handle commas.
758516	FortiAuthenticator HA: cluster out of sync if the custom RADIUS dictionary is uploaded; authentication breaks.
761880	Support FortiToken Cloud user for OAuth authentication.
766379	Pending or deleted CSR and revoked certificates do not sync to the LB secondary.
770593	Minimize the use of CBC ciphersuites.
775083	FortiAuthenticator FSSO detects FortiAuthenticator domain-join as login event, resolves workstation name to 127.0.0.1 and forwards that login.
777359	User will not be deleted on FortiToken Cloud but deleted on FortiAuthenticator when calling the REST API endpoint: `api/v1/localusers/USERID/`.
778729	Creating users via REST API with ftk_only field gives 500 error on user page when enabling password authentication.
779771	500 internal error shows when editing the LDAP entry.
779796	SAML IdP proxy for Azure is not working with the current Azure Portal.
780611	Oauth Token API returns error when calling the API `/oauth/token/` with FortiToken Cloud user, but FortiToken Cloud had sent push to the FortiToken Mobile.
782176	Certificate sync doesn't work from HA cluster to the LB note.
782448	Force password change on next logon produces 403 forbidden with SAML login.
782799	FTC manual sync times out when user > 1000, but actually the users are synced.
782965	FortiAuthenticator certificate verification issues (LDAPS, 802.1x).
785164	Remote admin unable to create self-service portal security question.
785585	HA load balancing anomaly for the registered captive portal user.
785634	Remote user without any FIDO keys for a FIDO enabled portal is unable to change the password.
788819	FortiAuthenticator 6.4.1 LDAP filters not being applied when importing groups from *Fortinet SSO Methods* > *SSO* > *SSO groups*.

Bug ID	Description
789931	FIDO key registration does not work if FQDN contains uppercase letters.
792031	SAML IdP with LDAP for Google SP randomly fails with Internal Server Error (Error 500).
792230	Encoding Migration Error after upgrading to 6.4.0 - 6.4.2 - no space left on device.
792723	FortiAuthenticator - Internal Server Error - Table `fac_auth_facgroup` is replicated and cannot be modified on a subscriber node.
793478	SAML SSLVPN authentication fails because FortiAuthenticator cuts parts of the DN when using the group LDAP filter.
793627	SAML sync rule shows javascript error.
793837	500 error when clicking on revoked and expired server certificate.
793868	Onboarding message feature sends SMS via unexpected SMS gateway.
794167	Self-service portal: Token revocation error.
794222	GUI crashes when we try to create a realm that already exists.
794681	FortiToken mobile 'Scan QR code' does not display the QR code for the remote SAML user.
794689	Refresh FortiToken Mobile button deprovisions FortiToken Mobile from the remote SAML user.
795030	Sponsor email address does not appear in recipient section of registration approval request email sent to freeform admin anymore.
795097	500 Internal Server Error when resetting the password.
795155	FortiAuthenticator API not performing input validation on the groups.
795275	Issues after upgrading from 6.0.7 to 6.4.2.
795560	SmartConnect profile generating certificate with incorrect suffix.
795939	When mschapv2 is used between FortiAuthenticator and FortiGate, the portal login is broken.
796079	RADIUS server stops responding to access requests in a very busy environment.
796431	SNMP api 'auth_failure' should be renamed to 'auth_failures'.
796844	Cancel button not working when editing local or remote user after upgrading to 6.4.2 or 6.4.3.
796891	FortiAuthenticator as IdP, using custom att splits `<saml:Attribute Name='username'>` into multiple lines.
797216	Not possible to add realm to IdP definition without a valid license in 6.4.3.
797870	Show disconnects admin from the CLI.
797909	Execution of sync rule runs FortiToken Cloud synchronization for all FortiAuthenticator users if user is removed from FortiAuthenticator as a result of sync rule.
798099	500 internal server error when trying to display Oauth sessions.
799416	[3rd party component upgrade required for security reasons] FortiAuthenticator - pillow to 9.0.1.

Bug ID	Description
799762	FortiAuthenticator cluster - CLI system time on secondary does not match primary.
799785	'Test Token' option under individual users doesn't have the country code selected.
799792	[3rd party component upgrade required for security reasons] FortiAuthenticator - curl to 7.83.1.
801043	nslookup broken: nslookup: applet not found.
801589	OpenID Missing Issuer URL.
801764	REST API Put request for usergroup gets 500 error.
803568	REST API authentication with password for ftk_only users fails in these two special cases
803891	SAML peer certificate expiration issue and XML security issue.
804229	SAML usernames are case sensitive, resulting in a failure of FortiToken assignment.
805371	FortiAuthenticator 6.4.3 - 802.1X RADIUS service restarted after certificate binding process.
805720	[3rd party component upgrade required for security reasons] FortiAuthenticator - linux_kernel to 5.10.111/5.4.189/4.19.238/4....
806115	Username/Email is not auto-populated after SAML redirection from SP (O365) to IdP (FortiAuthenticator).
807151	Self-Service portal replacement template for FortiToken Mobile activation Scan QR Message does not reflect the changes.
807153	No Replacement Message template for 'FortiToken Mobile Activation Scan QR Message' for Legacy Self Service Portal.
813480	Rebooting the FortiAuthenticator causes OAuth service to stop working - returns 500 server error.

Known issues

This section lists the known issues of this release, but is not a complete list. For inquires about a particular bug, please visit the Fortinet Support website.

Bug ID	Description
506112	This post Rest API call fails to activate FortiGuard messaging license.
540551	Should automatically pick up configured IP address on ports other than port1 for Azure cloud FortiAuthenticator.
561506	RADIUS authentications fail if no port on FortiAuthenticator is assigned an IPv4 address.
566145	Usage Profile `'TIME USAGE=Time used'` is not triggering COA or disconnect request to FortiGate.
581065	SAML users from downloading user audit csv file 'last used' field is empty.
646299	Nutanix AHV KVM based Hypervisor FortiAuthenticator upgrades from 6.0.4 to 6.1.x fail hangs on 'Waiting for Database'.
660918	Clicking the *Allow remote LDAP groups* button in RADIUS or TACACS policy reverts all the selected groups.
660921	Guest portal should not work if the URL contains http instead of https.
674164	Logging in to the CLI with incorrect password on the HA secondary gives a bunch of SQL errors.
676532	When FortiAuthenticator has RADIUS Client set as subnet, RADIUS accounting disconnect messages are not sent.
676985	Unable to import all FTK hardware tokens from the same purchase order; need to add them all manually.
680776	AP HA secondary cannot change mgmt interface access configuration, and the option does not sync from the primary either.
685172	FortiAuthenticator A-P running in v6.2.1 does not sync with the secondary unit pre-authentication warning message, CLI and GUI Timeout.
689458	HA cluster changing secret on the primary to match the secondary causes the webserver to crash on the secondary.
717191	SNMP traps generation issues.
723677	Failed auth after changing port on secure LDAP server locks radiusd and prevents it from being killed.
743775	SCEP Get CA requests intermittently fails under High Scep Load.
751108	FortiAuthenticator does not support admin OIDs from FORTINET-CORE-MIB properly.
767935	A-P cluster, it forms when configured from the GUI, it does not when configured from the CLI without a restart.
773020	Revoking of certificate is not being seen with OCSP until FortiAuthenticator reboots.
781832	Token bypass not working for FIDO enabled self-service portal.

Bug ID	Description
787013	Changing the username attribute will cause the remote sync rule to remove the existing remote users and eventually reimport them.
787156	FortiAuthenticator 6.4.1 GA OIDC HTTP Error 500.
789933	GUI access should be allowed for IP set on any interface.
791127	Sometimes(randomly) FortiAuthenticator fails to send email notification.
791347	Internal server error 500 happens when viewing RADIUS account sessions, probably caused by the `Called-Station-Id` attribute.
793191	Override Session.
793838	Password not defined after importing users from LDAP as a local user via a sync rule.
795924	SMS messages being sent through FortiGuard server always shows log error.
795938	Sponsors that try to access other Sponsor's guest users information get 500 error.
796156	SNMP table thresholds should not be able to exceed 100 percent.
796493	LDAPS connectivity issue between FortiGate/FortiManager and FortiAuthenticator.
799595	LDAP users with long DN cannot log in to the self-service portal.
799641	FIDO key user should have information in *User Lookup*.
799675	Fine Grained Controls are not working for the self-service portal.
799768	Automatic CRL download error with 2 Identical DN.
800674	Remote sync rule does not automaticaly apply FortiToken logo to remote SAML users.
801009	Remote SAML user sync rule creates one log entry for every SAML user assgined FortiToken Mobile every time the SAML sync occurs.
801445	FortiToken Mobile in pending state stays pending forever after deleting associated user which means we cannot use that FortiToken Mobile any longer.
801933	FortiAuthenticator as LDAP server, logs shows LDAP_FAC in 'Source IP' field.
806837	FortiAuthenticator license file too large for AWS.
807527	Import the same yubiken token cvs file twice will cause 500 error.
808310	Password reset crashes after "n" attempts on security question where "n" is the number specified in the lockout policy.
808327	After one incorrect security question answer, user status changes to 'Temporarily locked'.
809353	Country code selection for guest portal user registration on iOS selects incorrect country prefix.
810530	FortiAuthenticator FSSO user capacity in GUI on FAC 3000D is wrong.
811255	Lost my token option displaying 'string index out of range' error.
811368	Remote user sync rule not binding all certificates to the users.

Bug ID	Description
811662	FortiAuthenticator IdP, erorr 403 when returning to the SP after registering on a self-service portal.
812240	Making changes from trusted admin does not work.
813844	SYN packet sent outside zero trust tunnel when creating remote LDAP server with zero trust tunnel.

Maximum values for hardware appliances

The following table lists the maximum number of configuration objects per FortiAuthenticator appliance that can be added to the configuration database for different FortiAuthenticator hardware models.

Similar to the FortiAuthenticator-VM, the FortiAuthenticator hardware appliances permit stacking licenses.

The maximum values in this document are the maximum configurable values and are not a commitment of performance.

Feature		Model							
		200E	300F	400E	800F	1000D	2000E	3000E	3000F
System									
Network	Static Routes	50	50	50	50	50	50	50	50
Messages	SMTP Servers	20	20	20	20	20	20	20	20
	SMS Gateways	20	20	20	20	20	20	20	20
	SNMP Hosts	20	20	20	20	20	20	20	20
Administration	Syslog Servers	20	20	20	20	20	20	20	20
	User Uploaded Images	40	90	115	415	515	1015	2015	2015
	Language Files	50	50	50	50	50	50	50	50
Realms		20	60	80	320	400	800	1600	1600
Authentication									
General	Auth Clients (NAS)	166	500	666	2666	3333	6666	13333	13333

Feature	Model							
	200E	300F	400E	800F	1000D	2000E	3000E	3000F
Users (Local + Remote)[1]	500	1500/3500*	2000	8000/18000*	10000	20000	40000	40000/240000*
User RADIUS Attributes	1500	4500	6000	24000	30000	60000	120000	120000
User Groups	50	150	200	800	1000	2000	4000	4000
Group RADIUS Attributes	150	450	150	2400	600	6000	12000	12000
FortiTokens	1000	3000	4000	16000	20000	40000	80000	80000
FortiToken Mobile Licenses[2]	200	200	200	200	200	200	200	200
LDAP Entries	1000	3000	4000	16000	20000	40000	80000	80000
Device (MAC-based Auth.)	2500	7500	10000	40000	50000	100000	200000	200000
RADIUS Client Profiles	500	1500	2000	8000	10000	20000	40000	40000
Remote LDAP Servers	20	60	80	320	400	800	1600	1600
Remote LDAP Users Sync Rule	50	150	200	800	1000	2000	4000	4000
Remote LDAP User Radius Attributes	1500	4500	6000	24000	30000	60000	120000	120000

Feature		Model							
		200E	300F	400E	800F	1000D	2000E	3000E	3000F
FSSO & Dynamic Policies									
FSSO	FSSO Users	500	1500	2000	8000	10000	20000	200000[3]	200000
	FSSO Groups	250	750	1000	4000	5000	10000	20000	20000
	Domain Controllers	10	15	20	80	100	200	400	400
	RADIUS Accounting SSO Clients	166	500	666	2666	3333	6666	13333	13333
	FortiGate Services	50	150	200	800	1000	2000	4000	4000
	FortiGate Group Filtering	250	750	1000	4000	5000	10000	20000	20000
	FSSO Tier Nodes	5	15	20	80	100	200	400	400
	IP Filtering Rules	250	750	1000	4000	5000	10000	20000	20000
Accounting Proxy	Sources	500	1500	2000	8000	10000	20000	40000	40000
	Destinations	25	75	100	400	500	1000	2000	2000
	Rulesets	25	75	100	400	500	1000	2000	2000
Certificates									
User Certificates	User Certificates	2500	7500	10000	40000	50000	100000	200000	200000
	Server Certificates	50	150	200	800	1000	2000	4000	40000

Feature		Model							
		200E	300F	400E	800F	1000D	2000E	3000E	3000F
Certificate Authorities	CA Certificates	10	10	10	50	50	50	50	50
	Trusted CA Certificates	200	200	200	200	200	200	200	200
	Certificate Revocation Lists	200	200	200	200	200	200	200	200
SCEP	Enrollment Requests	2500	7500	10000	40000	50000	100000	200000	200000

[1] Users includes both local and remote users.

[2] **FortiToken Mobile Licenses** refers to the licenses that can be applied to a FortiAuthenticator, not the number of FortiToken Mobile instances that can be managed. The total number is limited by the FortiToken metric.

[3] For the 3000E model, the total number of concurrent SSO users is set to a higher level to cater for large deployments.

* Upper limit

Maximum values for VM

The following table lists the maximum number of configuration objects that can be added to the configuration database for different FortiAuthenticator virtual machine (VM) configurations.

The maximum values in this document are the maximum configurable values and are not a commitment of performance.

The FortiAuthenticator-VM is licensed based on the total number of users and licensed on a stacking basis. All installations must start with a FortiAuthenticator-VM Base license and users can be stacked with upgrade licenses in blocks of 100, 1,000, 10,000 and 100,000 users. Due to the dynamic nature of this licensing model, most other metrics are set relative to the number of licensed users. The **Calculating metric** column below shows how the feature size is calculated relative to the number of licensed users for example, on a 100 user FortiAuthenticator]-VM Base License, the number of auth clients (RADIUS and TACACS+) that can authenticate to the system is:

100 / 3 = 33

Where this relative system is not used e.g. for static routes, the **Calculating metric** is denoted by a "**-**". The supported figures are shown for both the base VM and a 5000 user licensed VM system by way of example.

Feature		Model			
		Unlicensed VM	Calculating metric	Licensed VM (100 users)	Example 5000 licensed user VM
System					
Network	Static Routes	2	50	50	50
Messaging	SMTP Servers	2	20	20	20
	SMS Gateways	2	20	20	20
	SNMP Hosts	2	20	20	20
Administration	Syslog Servers	2	20	20	20
	User Uploaded Images	19	Users / 20	19 (minimum)	250
	Language Files	5	50	50	50
Authentication					
General	Auth Clients (RADIUS and TACACS+)	3	Users / 3	33	1666

Feature		Model			
		Unlicensed VM	Calculating metric	Licensed VM (100 users)	Example 5000 licensed user VM
User Management	Authentication Policy (RADIUS and TACACS+)	6	Users	100	5000
	Users (Local + Remote)[1]	5	**********	100	5000
	User RADIUS Attributes	15	Users x 3	300	15000
	User Groups	3	Users / 10	10	500
	Group RADIUS Attributes	9	User groups x 3	30	1500
	FortiTokens	10	Users x 2	200	10000
	FortiToken Mobile Licenses (Stacked) [2]	3	200	200	200
	LDAP Entries	20	Users x 2	200	10000
	Device (MAC-based Auth.)	5	Users x 5	500	25000
	Remote LDAP Servers	4	Users / 25	4	200
	Remote LDAP Users Sync Rule	1	Users / 10	10	500
	Remote LDAP User Radius Attributes	15	Users x 3	300	15000
FSSO & Dynamic Policies					

Feature		Model			
		Unlicensed VM	Calculating metric	Licensed VM (100 users)	Example 5000 licensed user VM
FSSO	FSSO Users	5	Users	100	5000
	FSSO Groups	3	Users / 2	50	2500
	Domain Controllers	3	Users / 100 (min=10)	10	50
	RADIUS Accounting SSO Clients	10	Users	100	5000
	FortiGate Services	2	Users / 10	10	500
	FortiGate Group Filtering	30	Users / 2	50	2500
	FSSO Tier Nodes	3	Users /100 (min=5)	5	50
	IP Filtering Rules	30	Users / 2	50	2500
	FSSO Filtering Object	30	Users x 2	200	10000
Accounting Proxy	Sources	3	Users	100	5000
	Destinations	3	Users / 20	5	250
	Rulesets	3	Users / 20	5	250
Certificates					
User Certificates	User Certificates	5	Users x 5	500	25000
	Server Certificates	2	Users / 10	10	500
Certificate Authorities	CA Certificates	3	Users / 20	5	250
	Trusted CA Certificates	5	200	200	200
	Certificate Revocation Lists	5	200	200	200
SCEP	Enrollment Requests	5	Users x 5	500	25000

[1] Users includes both local and remote users.

[2] **FortiToken Mobile Licenses** refers to the licenses that can be applied to a FortiAuthenticator, not the number of FortiToken Mobile instances that can be managed. The total number is limited by the FortiToken metric.

www.fortinet.com